METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR SELECTIVELY ALLOWING USERS OF A MULTI-USER SYSTEM ACCESS TO NETWORK RESOURCES

FIELD OF THE INVENTION

The present invention relates to multi-user computer systems and, more particularly, to operations for controlling access by users of a multi-user system to resources within a network.

5

BACKGROUND OF THE INVENTION

Networks in which a plurality of computers and other electronic devices are inter-connected by wired or wireless communications links to facilitate

10 communications between users and/or the sharing of resources, (e.g., hardware, software, data sets, etc.) are known in the art. One well known type of network is an internet protocol or "IP" network which operates under the IP protocol that has been developed to

15 control communications sent over the Internet. Networks operating under the IP protocol typically include large numbers of geographically dispersed devices that are interconnected by a plurality of communications links and network routing and control

20 resources. A wide variety of different devices may be

included in the network, including, for example, mainframe computers, file servers, personal computers, printers, work stations, scanners, personal data assistants, cellular telephones, etc. Data processing devices such as, for example, mainframe computers that are part of the network may often be accessed by a plurality of users in the network.

Each device in the IP network is typically assigned an IP address. Communications packets sent over the IP network typically include headers that provide various information regarding the source and intended destination of the packet. This information may include, for example, the IP addresses of the source and/or destination devices, protocol and port information, and various other information which is well known to those of skill in the art.

In many instances, access to certain devices (e.g., computers, routers, printers, etc.) in an IP network may be restricted such that certain users are not permitted to access these resources. To provide such controlled access, an IP network may include "firewalls" which use packet level filtering to control access to devices in the IP network. Firewalls may be implemented at host devices and examine the IP source address, protocol, port and/or other information included in each received packet to determine if the packet will be processed by the host device. Firewalls may also be implemented at points of entry to specific sub-networks that have different security requirements than the IP network as a whole. Thus, for example, a firewall may be placed at a local area network server to restrict the access of those outside the local area network to devices within the local area network.

Firewalls, however, may not provide an effective method of controlling access to network devices in all

situations. Accordingly, there is a need for improved methods and systems of controlling user access to devices in an IP network.

SUMMARY OF THE INVENTION

Embodiments of the present invention include methods, systems and computer program products for selectively allowing a user of a multi-user system access to a plurality of resources in a network. Pursuant to these methods, systems and computer program products, a request, originated by a user of the multi-user system, may be received to transmit a message over the network to one of the plurality of resources in the network. A security zone associated with this resource may then be identified. Pursuant to the operations of the present invention, if it is determined that the user is authorized access to the identified security zone, the message may be forwarded over the network to the resource.

In embodiments of the present invention, a security zone may be associated with each of the plurality of resources in the network. Operations may also be provided for specifying the security zones to which particular users of the multi-user system are authorized access. The operations for identifying the security zone associated with the resource may comprise accessing a data structure that specifies the security zone associated with each resource in the plurality of resources.

In further embodiments of the present invention, at least one entry in the data structure may specify the security zone associated with a group of the resources in the plurality of resources. In these embodiments, the step of identifying the security zone associated with the one of the plurality of resources

may comprise identifying the security zone associated with the most specific entry in the data structure that includes the resource. The multi-user system may perform the operations for identifying the security zone associated with a resource in the network and determining whether a particular user is authorized access to the identified security zone.

Methods, systems and computer program products are also provided for determining whether to allow an operation associated with a user identification corresponding to a user of a multi-user system that involves access to a resource in a network. Pursuant to these methods, systems and computer program products (i) the resources in the network may each be classified as being associated with a particular security zone, and (ii) the security zones to which each user identification may have access may be specified. An operation may then only be allowed if the user identification is specified as having access to the security zone associated with the network resource which is to be accessed in the operation.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a network environment in which the present invention may be implemented;

Figure 2 illustrates the network environment of **Figure 1** wherein the network has been divided into a plurality of security zones;

Figure 3 is a block diagram of aspects of an S/390 computer system which may be used to implement the operations of embodiments of the present invention;

Figure 4 is a block diagram of an implementation of the network access data structure according to embodiments of the present invention; and

Figure 5 is a block diagram of an implementation of the security database according to embodiments of the present invention;

Figure 6 is a flowchart illustrating operations according to embodiments of the present invention; and

Figure 7 is a flowchart illustrating operations according to further embodiments the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention now will be described more fully hereinafter with reference to the accompanying drawings, in which preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art.

As will be appreciated by one of skill in the art, the present invention may be embodied as a method, data processing system, and/or computer program product. Accordingly, the present invention may take the form of an entirely hardware embodiment, an entirely software embodiment or an embodiment combining software and hardware aspects. Furthermore, the present invention may take the form of a computer program product on a computer-usable storage medium having computer-usable program code means embodied in the medium. Any suitable computer readable medium may be utilized including hard disks, CD-ROMs, optical storage devices,

a transmission media such as those supporting the Internet or an intranet, or magnetic storage devices.

Computer program code for carrying out operations of the present invention may be written in conventional procedural programming languages, such as, for example, the "C" programming language or PL/X. However, the computer program code for carrying out operations of the present invention may also be written in an object oriented programming language such as Java®, Smalltalk or C++. The program code may execute entirely on a single computer, or be distributed so as to execute on a plurality of computers and/or other data processing devices.

The present invention is described below with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions specified in the flowchart and/or block diagram block or blocks.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory

produce an article of manufacture including instruction means which implement the function specified in the flowchart and/or block diagram block or blocks.

The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart and/or block diagram block or blocks.

The present invention relates to methods, systems and computer program products for controlling user access to "resources" in a computer network such as an internet protocol ("IP") network. In particular, the present invention provides mechanisms for limiting the access of "users" of a "multi-user system" to resources in the network in situations where some, but not others, of the users of the multi-user system should be allowed access to the network resources that are to be protected.

As will be appreciated by those of skill in the art, typically a number of different persons and/or devices access and use the mainframe computer or other data processing device associated with a multi-user system. Each such person or device will normally have its own (or a shared) "user identification." The persons/devices accessing the data processing device may be resident at the data processing device, connected by a hard-wired connection, connected via a network connection, or connected via a variety of other connections.

Typically, a user identification is associated with each application being executed at any given time

on the data processing device. As noted above, such a
user identification could be associated with a person
resident at the data processing device or,
alternatively, with a person accessing the data
5   processing device from thousands of miles away over a
network connection. Likewise, the user identification
may be associated with a person or group of persons or,
alternatively, may be associated with a device or group
of devices. As used herein, the term "user" refers to
10   the person(s) and/or device(s) associated with a
particular user identification, and the term "multi-
user system" refers to a computer or other data
processing device which more than one user may use to
execute applications. However, since each application
15   executing on a multi-user system is generally
associated with some user identification, the term
"user" may likewise be viewed as referring to a piece
of work executing on the multi-user system (since it is
understood that there is a user identification that is
20   associated with that piece of work).

     As will be appreciated by those of skill in the
art, a wide variety of different computers, printers,
file servers, web servers, data processing devices,
etc. can be interconnected in a network, and that these
25   devices may further include, or be connected to,
additional devices such as disk drives, modems,
printers, etc. It will be understood that as used
herein, the term "resource" refers to any separately
addressable entity in the network. Thus, for example,
30   in an IP network, a resource refers to any device in
the network having its own IP address.

     Embodiments of the present invention will now be
described with reference to an IP network. However, it
will be appreciated that the methods, systems and
35   computer program products of the present invention are

equally applicable to other types of networks, such as, for example, local area networks or networks operating under the Systems Network Architecture ("SNA") protocol.

5   As noted above, in conventional IP networks, firewalls that implement host-based packet filtering are typically provided to control access to resources within the IP network. These firewalls examine parameters such as the source IP address, port number,

10   protocol, etc. specified in individual data packets to evaluate whether or not the packet should be forwarded beyond the firewall. However, when a data packet is originated and transmitted over the network by a multi-user system, the source IP address, port number,

15   protocol and other potential identification parameters may be the same for all packets sent by the multi-user system, regardless of which particular user of the multi-user system originated the packet. Consequently, traditional firewalls may not be an effective mechanism

20   for selectively allowing the users of such multi-user systems access to resources in the IP network.

     An example of a multi-user system is an IBM S/390 mainframe computer that serves as a portal to an IP network for a plurality of user workstations and

25   applications. Each workstation may be accessed by one or more different users, and additional users in the network may access and execute software applications on the S/390 mainframe computer via a network, Telnet or other connection. It will be understood that numerous

30   other multi-user systems are commonly connected to IP networks, such as various server platforms manufactured by Hewlett Packard and Sun, local area networks operating under Windows NT, etc. When such multi-user systems are included in, or have access to, the IP

35   network, conventional host-based firewalls may not

provide a mechanism for selectively allowing and restricting access by users of the multi-user system to resources in the IP network.

Pursuant to the teachings of the present invention, methods, systems and computer program products for controlling user access to the IP network at the multi-user system are provided. The approach of the present invention for controlling user access to IP network resources may be combined with conventional IP network security mechanisms, such as packet filtering firewalls, to provide a fully secure networking environment. Thus, the methods, systems and computer program products of the present invention may be used locally, at the multi-user system, to restrict user access to resources in the IP network, while the firewalls can be used within the IP network to globally restrict access to network resources based on criteria such as source IP address.

Referring first to **Figure 1**, an IP network environment in which embodiments of the present invention may be implemented will be generally described. The IP network **10** of **Figure 1** is provided for illustrative purposes only, and those of skill in the art will appreciate that a typical IP network may include thousands of users, and include a wide variety of network resources and devices. As illustrated in **Figure 1**, the IP network **10** includes a plurality of mainframe computers **20, 21, 22,** routers **30, 31, 32, 33** and workstations **40, 41, 42, 43, 44, 45, 46, 47, 48, 49** interconnected by network communications links. As shown in **Figure 1,** the workstations **40-49** may either have direct access to the IP network **10,** or may access other resources in the IP network **10** via one or more of the mainframe computers **20-22.**

As noted above, a "multi-user system" refers to a computer or other data processing device which may execute applications associated with more than one user. In **Figure 1,** each of the mainframe computers **20-22** comprise such a multi-user system, as might additional of the workstations **40-49** depicted in **Figure 1** to the extent they likewise execute applications associated with more than one user.

Thus, it will be appreciated that virtually any device may act as a "multi-user system" and that the present invention is applicable to all types of multi-user systems, and not just systems with mainframe computers. To simplify the following discussion, mainframe computers **20-22** will be treated as the only multi-user systems in **Figure 1.**

In the IP network **10** of **Figure 1,** a software application or other piece of work executing on one of the mainframe computers **20** may generate a request to access another resource (e.g., mainframe computer **22**) in the IP network. While the software application running on the mainframe computer **20** will be associated with a particular user in the network (who might be resident at mainframe computer **20,** one of the attached workstations **40-42,** or at some other device in the network), typically, the connect call originated by the mainframe computer **20** to establish the connection with mainframe computer **22** will not specify the user identification associated with the application that caused the connect call to be originated. As a result, mainframe computer **22** (and other devices in network **10**) generally will not have knowledge as to which user caused the connect call to be generated, but instead will just know that the connect call was transmitted by mainframe computer **20.** In this situation, conventional

RSW920000155US1   -11-

firewalls may not be capable of allowing some of the users of mainframe computer **20** access to a resource in the network having heightened security requirements (*i.e.*, a resource which not every user or potential user of IP network **10** may access) while preventing other users of mainframe computer **20** access to such a restricted access resources.

Pursuant to the teachings of the present invention, the IP network **10** may be classified into "security zones" to facilitate allowing only selected users of a multi-user system such as mainframe computer **20** access to the restricted access network resources. A different security zone may be defined for each distinct level of security sensitivity required by the resources in IP network **10**. While a particular resource may be classified as belonging to multiple security zones, in embodiments of the present invention each network resource is classified as belonging to a single security zone. Network resources which are not classified as belonging to a security zone may be assigned to a default security zone.

Figure 2 illustrates one possible classification of security zones for the IP network **10** of **Figure 1**. In the example of **Figure 2**, each resource in the IP network **10** belongs to one of four different security zones, which are labeled as Zones A-D in **Figure 2**. As indicated in **Figure 2**, a particular security zone need not be contiguous, as typically network resources are assigned to security zones based on their security sensitivity and/or based on which users are allowed access to the resource.

In embodiments of the present invention, the classification of the IP network **10** into security zones may be performed by the security administrator for the

IP network **10**. However, this function could also be carried out by other individuals and/or resources in the network, including the system administrator for one of the multi-user systems, such as the system

5   administrator for one of the mainframe computers **20-22**. Moreover, in embodiments of the present invention, the multi-user system may perform the security zone classification of network resources for the purpose of limiting certain users of that particular multi-user

10   system access to resources in the IP network **10**. In such embodiments, no one outside the multi-user system may even be aware of the security zone classification.

    The security zone classification may be used to determine which users of one or more of the multi-user

15   systems may access which resources in the IP network **10**. This determination may be made, for example, by the security system, if provided, of a multi-user system such as mainframe computer **20**. By way of example, one known multi-user system is the S/390

20   mainframe computer manufactured by International Business Machines, Inc. of Armonk, New York. The operating system software, namely the OS/390, that is part of the S/390 system includes a security manager that has a Resource Access Control Facility or "RACF."

25   The RACF is designed to control access of users of the S/390 system to hardware and software within the S/390 system, and occasionally may also be used to control user access to external devices such as a printer. The RACF includes a database **132** that specifies the

30   hardware and software each user of the S/390 may access. This database is typically generated at installation, and updated as necessary thereafter. As described below, the RACF may be used according to embodiments of the present invention to control the

access that users of S/390 system are provided to
resources external to the S/390 in the IP network **10**.

Figure 3 is a block diagram of portions of an
S/390 system **100** in which an application **150** is being
run. In the example of **Figure 3**, the application **150**
is being run at the request of a user that is accessing
the S/390 system **100** via the workstation **110**. The
application **150** is generating communications that are
to be transmitted over an IP network **180**. As shown in
Figure 3, the S/390 system includes an OS/390 operating
system **120**, which includes a RACF **130**. In the example
of **Figure 3**, the application **150** is communicating over
the IP network **180** using a TCP/IP protocol. Thus, a
communications process such as the TCP/IP kernel **140** is
shown as being included in the operating system kernel
of the S/390 system **100**. It will be understood that
other kernel elements are typically also found on the
S/390 system **100**, which other kernel elements may
further support communications with applications over
the IP network **180** using other layered protocols.
Similarly, the communications process may be a
communications protocol stack, such as a TCP/IP
communications protocol stack, or such other process
which may be provided separate from the operating
system kernel but which may also provide for
controlling data transmission transaction requests
received from the application **150**.

During initialization of the TCP/IP kernel **140**, a
data structure **190** may be accessed that contains
information regarding the security zone to which each
resource in the TCP/IP network **180** belongs. By way of
example, this data structure **190** might contain the IP
address of each resource and/or group of resources in

the TCP/IP network **180,** along with the name (herein "zonename") of the security zone to which the resource or group of resources belongs.

In embodiments of the present invention, the data structure **190** may comprise a network resource-to-security zone mapping table **200** that similarly contains the IP address of each resource or group of resources in the TCP/IP network **180,** along with the zonename of the security zone to which the resource/group of resources belongs. **Figure 4** depicts such a mapping table **200.** As shown in **Figure 4,** the mapping table comprises an association between resources and groups of resources in the lefthand column with security zone classifications in the righthand column. In the example of **Figure 4,** the resources and groups of resources are specified using their IP address (which for ease of illustration are depicted as 8-bit addresses instead of as 32-bit addresses). In the data structure of **Figure 4,** entries in the mapping table specified by their full 8-bit address refer to a specific resource in the network. On the other hand, entries specified by less than 8-bits refer to all the resources which have the specified bits as the beginning portion of their IP address. To show this, the remaining bits are designated as "stars" to indicate that they may be either a zero or a one. As an example, the first entry in the data structure of **Figure 4** is 01011***. This entry refers to each of the eight resources (to the extent the resources are part of the IP network **180**) having an IP address beginning with the bits 01011. As shown in **Figure 4,** these eight resources are specified as belonging to security zone B.

As is also shown in **Figure 4**, a particular resource may appear to be specified as belonging to more than one security zone. For instance, the second entry in the data structure is 0101101*, which is

5   indicated as belonging to security zone A. Since the first five bits of this entry correspond to the five bits specified in the first entry in the data structure, it may appear that the resources 01011010 and 01011011 belong to both security zones A and B.

10   However, in situations where a resource (or group of resources) appears to be assigned to two or more different security zones, it may be treated as belonging to the security zone specified for the "most specific" entry in the mapping table **200**. The "most

15   specific" entry refers to the entry which refers to the smallest number of resources (*i.e.*, the entry in which the most bits of the IP address are not specified using wild card characters). Thus, in the data structure of **Figure 4**, the second entry is the most specific entry

20   for the resources 01011010 and 01011011, and hence they are classified as being part of security zone A.

The use of a mapping table such as the mapping table **200** depicted in **Figure 4** may provide for more efficient queries by the TCP/IP kernel **140** than

25   conventional look-up tables or other data structures. In particular, use of a mapping table such as the mapping table **200** depicted in **Figure 4** may allow for specifying the security zone associated with thousands of resources in the IP network with a relatively small

30   number of entries, but still provide complete flexibility as to which security zone a particular resource is assigned. The mapping table **200** may typically be accessed faster than a conventional look-

up table which does not group resources, and also typically requires less memory to store.

Referring back to **Figure 3,** in operation, when the application **150** transfers data to the TCP/IP kernel **140** for communications over the TCP/IP network **180,** the TCP/IP kernel **140** may look at the destination IP address designated for the data that is to be transmitted. The mapping table **200** may then be consulted by the TCP/IP kernel **140** to determine a zonename of the security zone that is associated with the most specific entry in the table that includes the resource corresponding to the designated destination address for the data. The TCP/IP kernel **140** may then access the data structure **132** in the RACF **130** to determine if the user associated with the application **150** is permitted access to the specified security zone. If access is permitted, the TCP/IP kernel **140** will allow the operation to proceed. If not, the TCP/IP kernel **140** will deny the requested operation. Thus, in this manner the TCP/IP kernel **140** may, in conjunction with the RACF **130,** serve to control the access of users of a multi-user system at the source of the potential security breach. Typically, the use of such an access control system would be added as an extra layer of protection, and thus would be used to augment, rather than replace, conventional security safeguards such as firewalls.

Figure 5 depicts an exemplary embodiment of the data structure **132** that specifies the resources each user of the S/390 may access. As shown in **Figure 5,** the data structure may be implemented as a simple look-up table that specifies the users (in the righthand column) that are permitted access to each security zone (which are listed in the lefthand column). It will be

appreciated that a wide variety of different data
structures may be used to store this information.

Pursuant to particular teachings of the present
invention, operations for determining how often
resource access checks are performed are also provided.
For instance, as is understood by those of skill in the
art, IP networks operating under a TCP transport layer
protocol build a connection each time a resource
communicates with another resource over the IP network.
As this connection carries all traffic between the
resources until termination of the connection, it may
not be necessary to perform a resource access check on
every packet that is to be forwarded across the network
over the connection. Instead, a resource access check
may be performed for an outbound connection during the
connect call. Resource access checks may or may not
then be performed on packets which are later sent over
the network via the connection. As will be understood
by those of skill in the art, one situation where it
may be desirable to re-perform a resource access check
on packets that are being transmitted over a TCP/IP
connection is where a user(s) associated with an
application changes while the application is still
running. If this occurs, it will typically be
desirable to re-perform the resource access check even
though a new connection has not been established.

Other transport layer protocols, however, such as
UDP and RAW, are connectionless protocols. With these
protocols, resource access checking may be performed
for every outbound packet that is to be transmitted.
However, even with these transport layer protocols it
will typically not be necessary to perform a resource
access check with respect to every packet, as a cache
memory often is available with information regarding
prior transmissions, and thus the cache may be checked

and the resource access check skipped in situations where a packet specifies the same source, destination and user identities as previous packets that were subject to a resource access check.

5   Typically, embodiments of the present invention only perform resource access checks on packets that originate within the multi-user system that are to be transmitted over the IP network, as packets that are merely being forwarded through the TCP/IP kernel **140** 10   have no associated user. Moreover, the security systems of the present invention may be established so that the IP layer does not require knowledge of the resource access check operations, as such operations may all be carried out at the transport layer.

15   Operations according to various embodiments of the present invention will now be described further with reference to the flowchart illustrations of **Figures 6-7**. Operations begin with reference to **Figure 6** at block **400** with an application that is running on the 20   multi-user system generating a request to transmit a packet over the IP network. While typically the software application that is running on the multi-user system generates this request, it will be understood that a user is associated with the application, and 25   thus the request may be viewed as having been "originated" by the particular user that is associated with the application. Once this request to transmit a packet is generated, as noted above, it is typically sent to a transport layer process such as TCP, UDP or 30   RAW. In response to the request, a network access data structure may be consulted to determine the security zone associated with the network resource to which the data is to be transmitted (block **402**). A user access database or other data structure may then be queried to

ascertain whether the user of the multi-user system associated with the application that forwarded the transmission request is allowed access to the security zone associated with the network resource with which it is attempting to communicate (block **404**). If the user is allowed access, the operation is allowed and the packet forwarded over the IP network (block **406**). If the user is not permitted access, the operation is denied (block **408**).

Figure 7 is a flow chart depicting operations according to additional embodiments of the present invention. As shown in **Figure 7**, each of a plurality of resources in an IP network may be classified as being associated with one of a plurality of security zones (block **500**). As discussed above, the classifications may be done on a resource-to-resource basis or may be done with respect to groups of resources or some combination thereof. Resources in the IP network need not be contiguous to be assigned to the same security zone. The security zone to which one or more of the users of the multi-user system may have access likewise may be specified (block **502**). This specification may be performed either before or after the resources in the IP network are classified as being associated with particular security zones. Once the above-mentioned operations have been completed, each time an application or other operation being run by a user of the multi-user system seeks to access or communicate with a resource in the IP network (block **504**), a determination may be made as to whether the resource which the user is seeking to access is associated with a security zone to which the user is specified as having access (block **506**). If it is, the operation is allowed (block **508**). If, on the other

hand, it is not, the operation is denied, and the user
is not permitted to access or communicate with the
resource (block **510**). If the resource is not specified
as being in any security zone (including the default
security zone, if any), the operation is allowed.

5

It will be appreciated that resources in the IP
network may be classified into specific security
"levels" or "zones" with respect to each different
multi-user system that is part of the IP network.
Thus, a particular network resource may, in certain
embodiments of the present invention, be part of a
first security zone that applies with respect to access
requests by users of a first multi-user system, and may
be part of a second security zone with respect to
access requests by users that are part of a second
multi-user system. This may, in certain circumstances,
simplify the classification process and limit the
number of different security zones which must be
specified. However, in other embodiments of the
present invention, the IP network resources may be
given a global security zone classification which is
used with respect to the users of all multi-user
systems that are part of the IP network.

10

15

20

As noted above, in certain embodiments of the
present invention, a security manager associated with
the multi-user system may be used to implement the
access control operations of the present invention.
One advantage of using such a security manager to
implement these operations is that little or no
software changes may be required to the security
manager. For example, by expanding the database
associated with the RACF on an OS/390 system to include
information regarding security zones as RACF resources
and which users of the multi-user system are permitted
access to such resources, the RACF may be used to

25

30

35

implement the access control operations of the present
invention. Moreover, in many instances, the security
manager of the multi-user system may provide
information (*e.g.*, a log of access requests that were
5   denied) that may be beneficial from an auditing
viewpoint.

The flowcharts and block diagrams of **Figures 3** and
6-7 illustrate the architecture, functionality, and
operation of possible implementations of systems,
10   methods and computer program products according to
various embodiments of the present invention. In this
regard, each block in the flow charts or block diagrams
may represent a module, segment, or portion of code,
which comprises one or more executable instructions for
15   implementing the specified logical function(s). It
should also be noted that, in some alternative
implementations, the functions noted in the blocks may
occur out of the order noted in the figures. For
example, two blocks shown in succession may, in fact,
20   be executed substantially concurrently, or the blocks
may sometimes be executed in the reverse order,
depending upon the functionality involved.

While the present invention has primarily been
described with respect to access control operations
25   that are performed on outbound data packets, it will be
appreciated that the operations specified herein may
also be modified to allow for access control checks on
inbound packets. By way of example (and with reference
to **Figure 3**), a data packet that is being forwarded
30   over the IP network to an application or process
running on the multi-user system may be received by the
TCP/IP kernel **140**. The TCP/IP kernel **140** may examine
the data packet to determine the resource in the IP
network that originally forwarded the packet, and may

use this information and a mapping table such as mapping table **200** to identify the security zone associated with that resource. The TCP/IP kernel **140** may then access the data structure **132** in the RACF **130**

5 to determine if the user associated with the application running on the multi-user system to which the data packet is being sent is authorized access to the security zone associated with the resource that transmitted the packet. If it is, the data packet is

10 forwarded to the local process or application; if it is not, the data packet is rejected.

In the drawings and specification, there have been disclosed typical preferred embodiments of the invention and, although specific terms are employed,

15 they are used in a generic and descriptive sense only and not for purposes of limitation, the scope of the invention being set forth in the following claims.